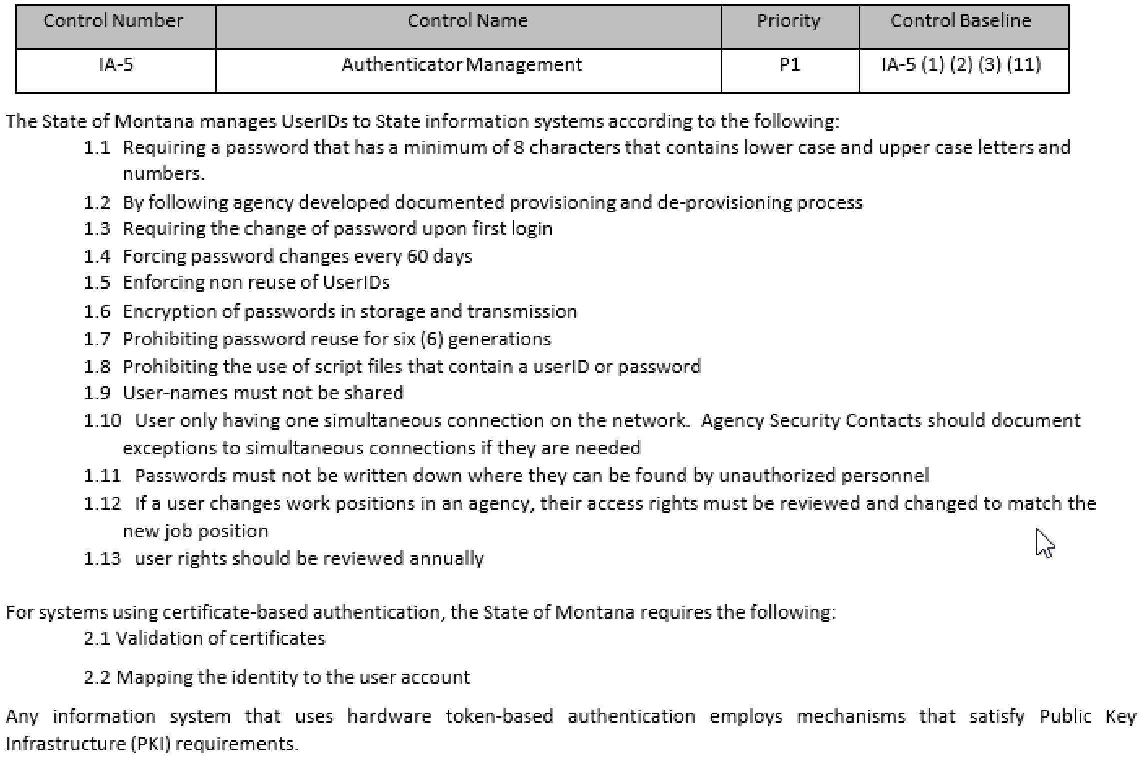
<u>MT-ISAC Best Practices Workgroup suggested edits to Appendix A based from Identification and Authentication Document.</u>



Control Number	Control Name	Priority	Control Baseline
IA-5	Authenticator Management	P1	IA-5 (1) (2) (3) (11)

The State of Montana manages UserIDs to State information systems according to the following:

1.1 Requiring a password that has a minimum of 8 characters that contains lower case and upper case letters and numbers.
1.2 By following agency developed documented provisioning and de-provisioning process
1.3 Requiring the change of password upon first login
1.4 Forcing password changes every 60 days
1.5 Enforcing non reuse of UserIDs
1.6 Encryption of passwords in storage and transmission
1.7 Prohibiting password reuse for six (6) generations
1.8 Prohibiting the use of script files that contain a userID or password
1.9 User-names must not be shared
1.10 User only having one simultaneous connection on the network. Agency Security Contacts should document exceptions to simultaneous connections if they are needed
1.11 Passwords must not be written down where they can be found by unauthorized personnel
1.12 If a user changes work positions in an agency, their access rights must be reviewed and changed to match the new job position
1.13 user rights should be reviewed annually

For systems using certificate-based authentication, the State of Montana requires the following:

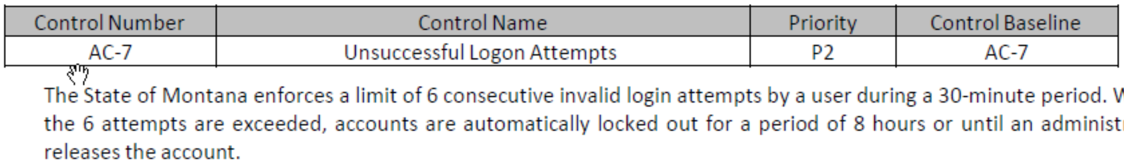
2.1 Validation of certificates

2.2 Mapping the identity to the user account

Any information system that uses hardware token-based authentication employs mechanisms that satisfy Public Key Infrastructure (PKI) requirements.

ID & Authentication Document recommends adding to IA-5 – Minimum age of password – 24 hours. This is a IRS Publication 1075 recommendation.

ID & Authentication Document recommends adding to IA-5 – Password for Elevated/Privileged/Administrative/SU Accounts should be at least 15 characters long.



Control Number	Control Name	Priority	Control Baseline
AC-7	Unsuccessful Logon Attempts	P2	AC-7

The State of Montana enforces a limit of 6 consecutive invalid login attempts by a user during a 30-minute period. When the 6 attempts are exceeded, accounts are automatically locked out for a period of 8 hours or until an administrator releases the account.

ID & Authentication Document is recommending changing from "locked out for a period of 8 hours" to "locked out for a period of 15 minutes". This is a IRS Publication 1075 recommendation.